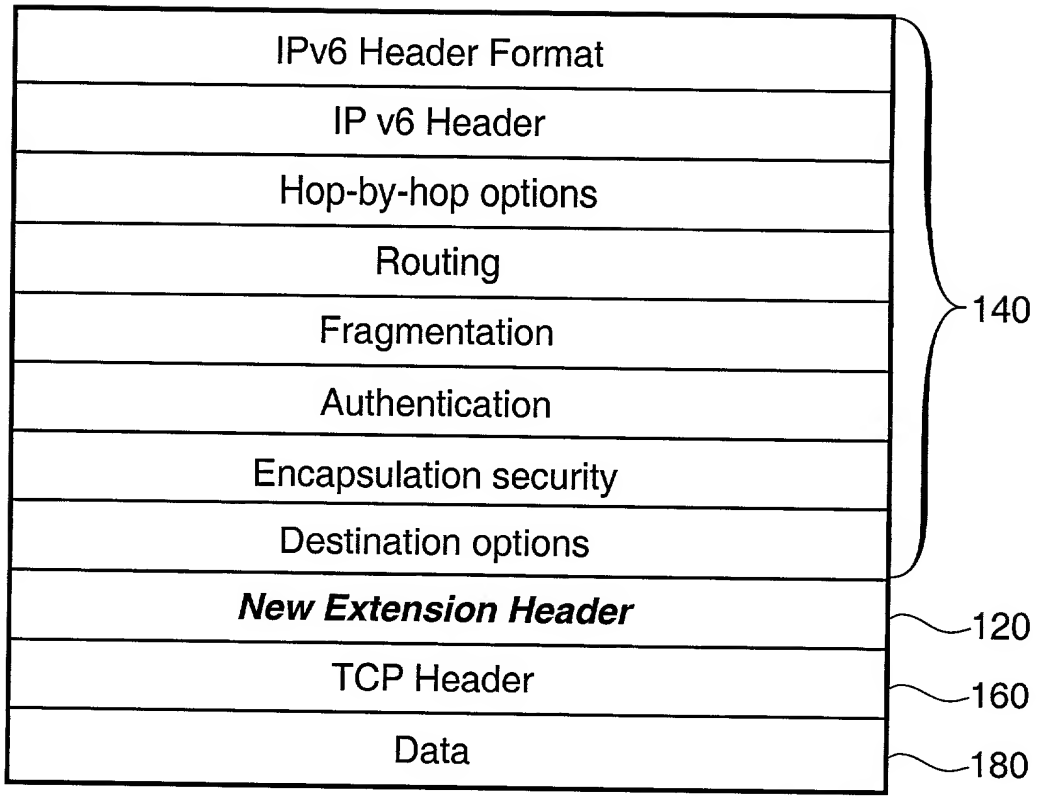
IPv6 Header Format
IP v6 Header
Hop-by-hop options
Routing
Fragmentation
Authentication
Encapsulation security
Destination options
New Extension Header
TCP Header
Data
140
120
160
180

Fig. 1

NEW EXTENSION HEADER FIELD NAME	MINIMUM SIZE	FIELD DESIGNATOR
Extension Header Size	128 bits	0 (zero)
Packet Type	2 bits	A
Requested Number of False Packets	8 bits	B
Minimum Hops for False Packets	8 bits	C
Minimum False Packet Body Size (Bytes)	32 bits	D
Maximum False Packet Body size (Bytes)	32 bits	E
Baseline False Packet Body Size (Bytes)	32 bits	F
True Packet (Message) Source Address	128 bits	G
Packet Body Re-encrytion Permitted	1 bit	H
False Packet Generation Probablity	8 bits	I
False Packet Generation Probablity Decay Rate	8 bits	J
Re-encryption Performed	1 bit	K
Re-encryption Probabilty	8 bits	L
Total number of Re-encryptions	32 bits	M
Decryption Key Pointer	128 bits per re-encryption	N

Fig. 2

	NEW EXTENSION HEADER FIELD NAME	MEANING	BIT DEFINITIONS
310	Extension Header Size	Size (in bits) of the new extension header within the current packet	N/A
312	Packet Type	Type of packet being transmitted	ØØ - True packet Ø1 - First generation false message packet 1Ø - Second or later generation false message packet. 11 - First generation false message packet generated by an intermediate host between originator and recipient of true message packet
314	Requested Number of False Packets	Number of first generation false packets requested to be generated by true message packet recipient	N/A
316	Minimum Hops for False Packet	Number of laps within the network that a false packet must complete	N/A
318	Minimum False Packet Body Size (Bytes)	Minimal size in bytes of the payload (data segment) in the packet for a false message packet	N/A
320	Maximum False Packet Body size (Bytes)	Maximum size in bytes of the payload (data segment) in the packet for a false message packet	N/A
322	Baseline False Packet Body Size (Bytes)	Actual size in bytes of the payload (data segment) in the true current message packet	N/A

Fig. 3

	NEW EXTENSION HEADER FIELD NAME	MEANING	BIT DEFINITIONS
324	True Packet Source Address	IPv6 address of the source of the true message packet	N/A
326	Re-encryption Permitted	Whether intermediate hosts can add a new level of encryption to packet by re-encrypting the body of the message packet	Ø - re-encryption is not permitted 1 - re-encryption is permitted
328	False Packet Generation Probablity	Binary value for the false packet generation probability	Ø - false packet generation probability is zero >Ø - false packet generation probability. Value is equal to 1 divided by the decimalized value of the bit representation
330	False Packet Generation Probablity Decay Rate	Binary value for the false packet generation probability decay rate	11111111- false packet generation probability is set to zero after generating one false packet. <11111111 - bit value to be added to False Packet Generation Probability value each time a false packet is generated at a host
332	Re-encryption Performed	Whether an intermediate host has re-encrypted the packet body	N/A
334	Re-encryption Probablity	Binary value for the probability that re-encryptionwill be performed on the packet	Ø - re-encryption probability is zero >Ø - re-encryption probability. Value is equal to 1 divided by the decimalized value of the bit representation
336	Total Number of Re-encryptions	A count of the number of reen-encryptions performed on a given packet as it moved through the network	N/A
338	Decryption Key Pointer	Designator for each decryption key needed to undo encryption applied by an intermediate host	N/A

Fig. 3A

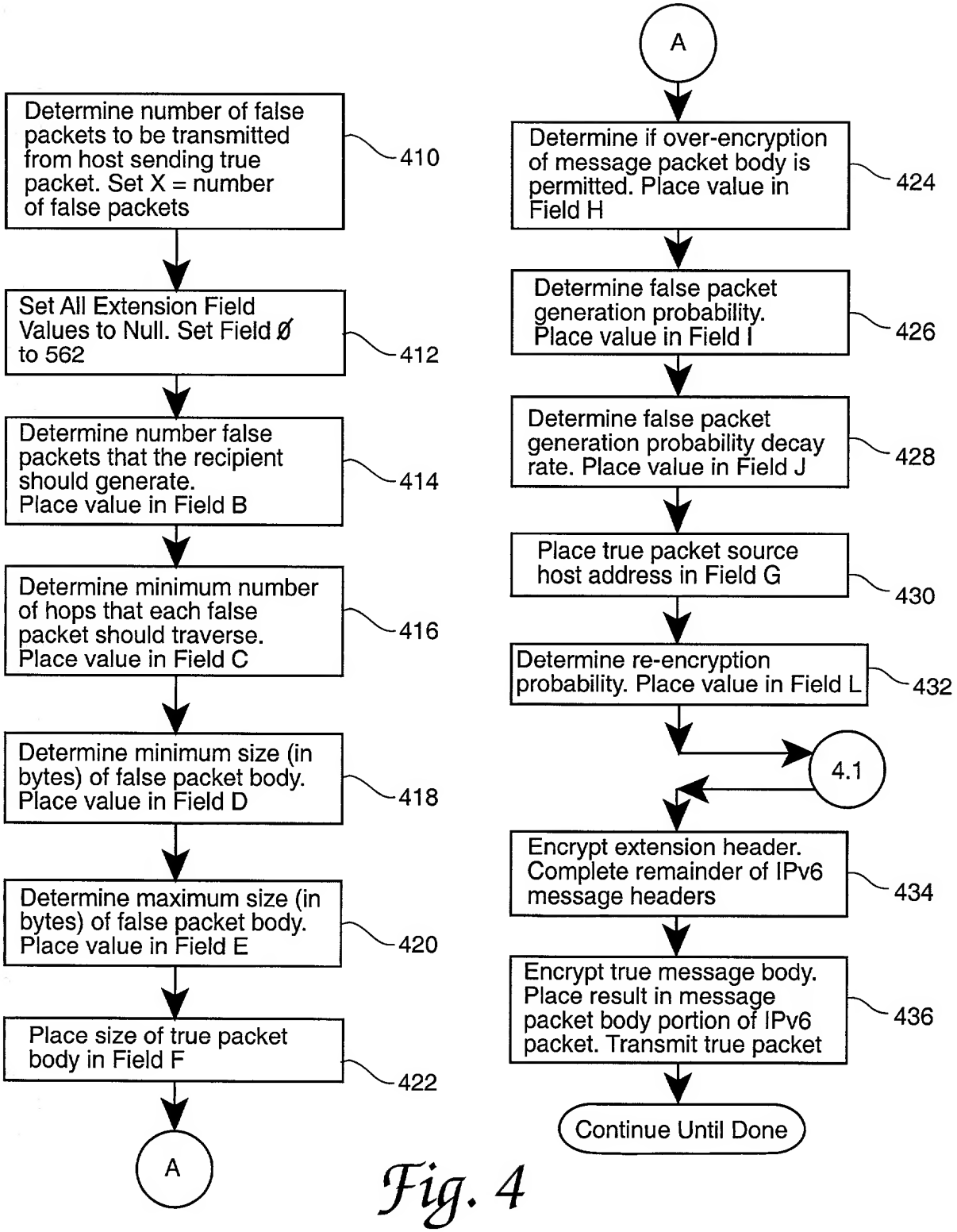
Determine number of false packets to be transmitted from host sending true packet. Set X = number of false packets
410
Set All Extension Field Values to Null. Set Field Ø to 562
412
Determine number false packets that the recipient should generate. Place value in Field B
414
Determine minimum number of hops that each false packet should traverse. Place value in Field C
416
Determine minimum size (in bytes) of false packet body. Place value in Field D
418
Determine maximum size (in bytes) of false packet body. Place value in Field E
420
Place size of true packet body in Field F
422
A
A
Determine if over-encryption of message packet body is permitted. Place value in Field H
424
Determine false packet generation probability. Place value in Field I
426
Determine false packet generation probability decay rate. Place value in Field J
428
Place true packet source host address in Field G
430
Determine re-encryption probability. Place value in Field L
432
4.1
Encrypt extension header. Complete remainder of IPv6 message headers
434
Encrypt true message body. Place result in message packet body portion of IPv6 packet. Transmit true packet
436
Continue Until Done

Fig. 4

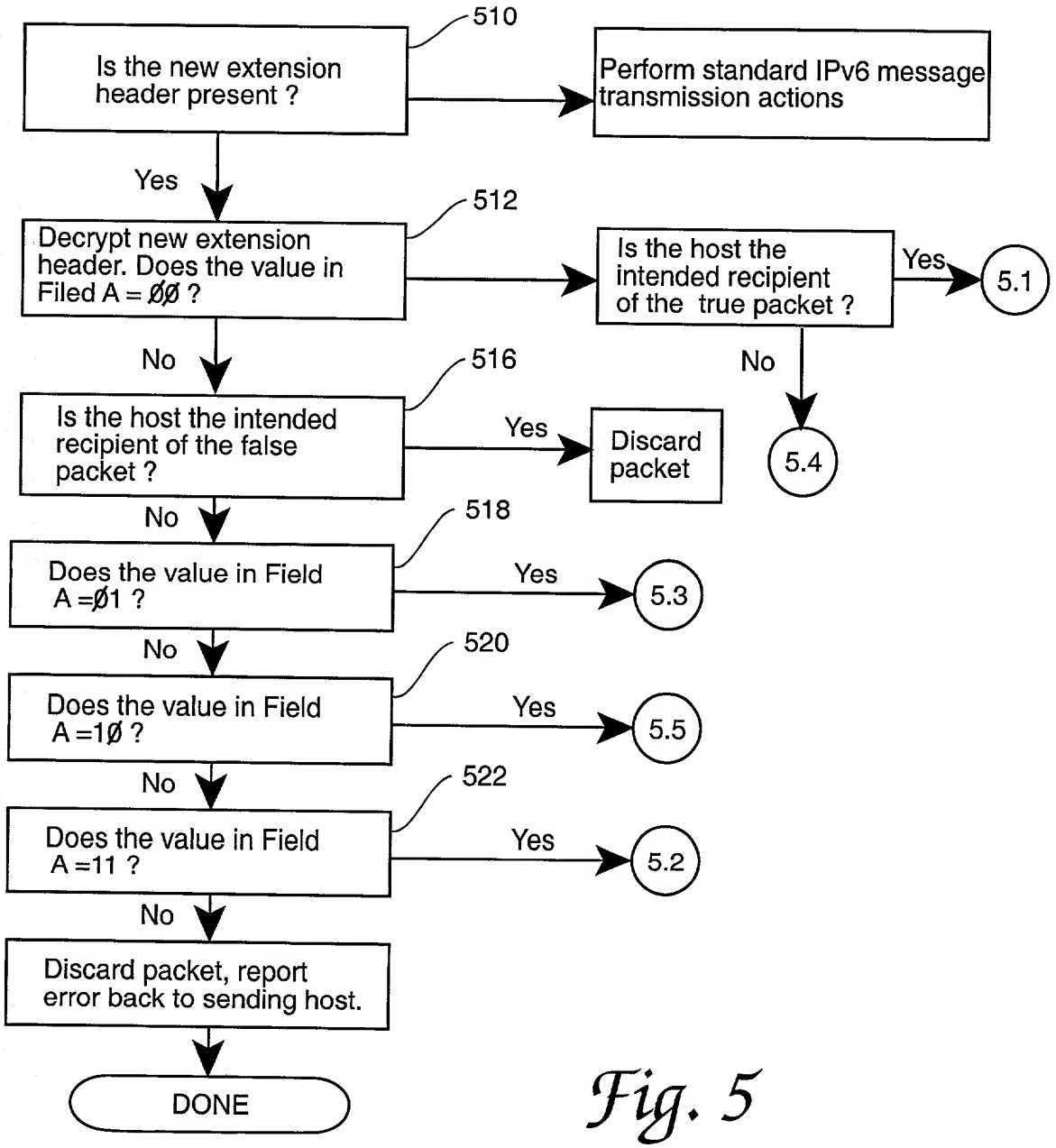
510
Is the new extension header present ?
Perform standard IPv6 message transmission actions
Yes
512
Decrypt new extension header. Does the value in Filed A = ØØ ?
Is the host the intended recipient of the true packet ?
Yes
5.1
No
No
516
Is the host the intended recipient of the false packet ?
Yes
Discard packet
5.4
No
518
Does the value in Field A =Ø1 ?
Yes
5.3
No
520
Does the value in Field A =1Ø ?
Yes
5.5
No
522
Does the value in Field A =11 ?
Yes
5.2
No
Discard packet, report error back to sending host.
DONE

Fig. 5

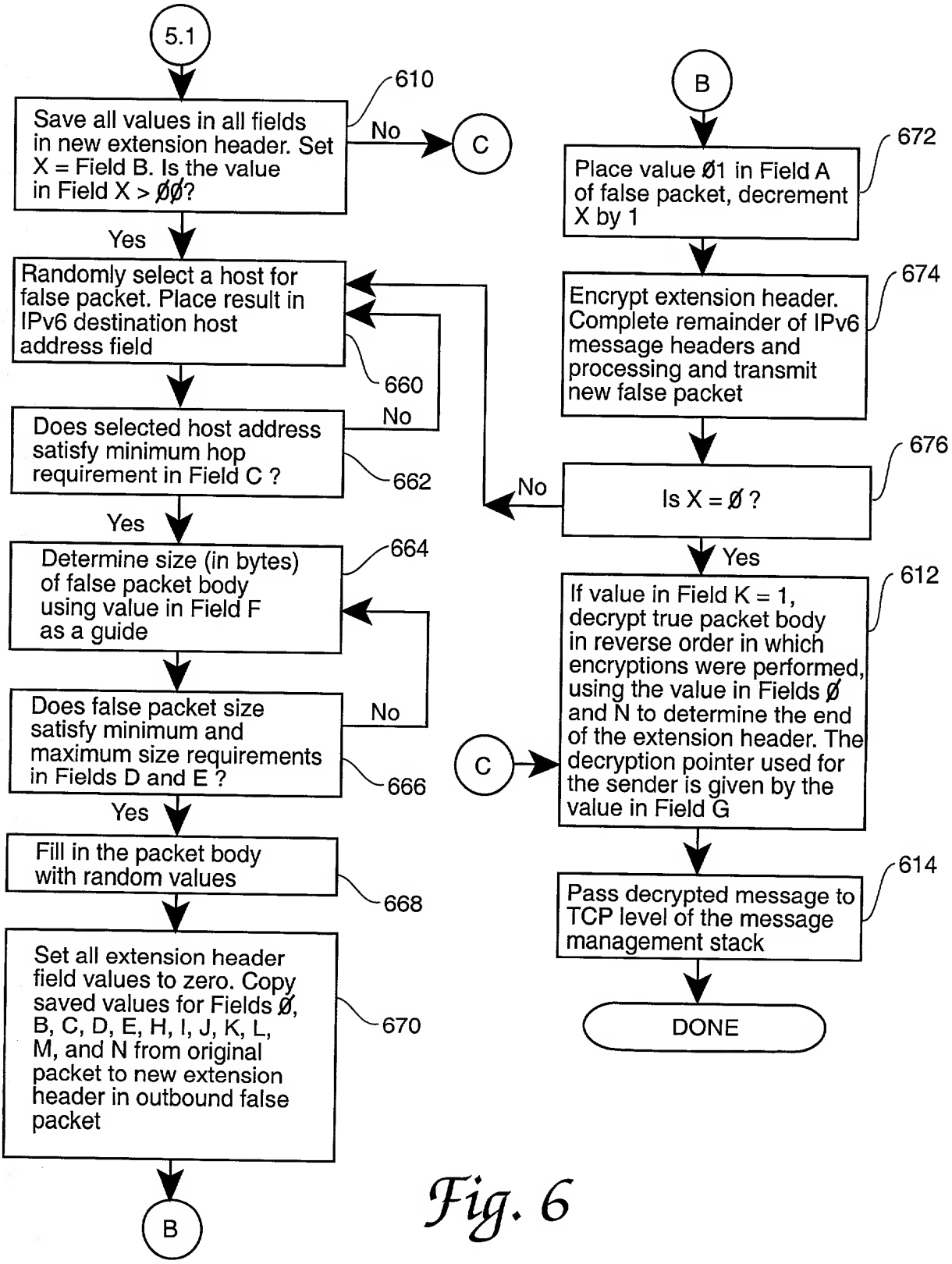
5.1
610
Save all values in all fields in new extension header. Set X = Field B. Is the value in Field X > ØØ?
No
C
Yes
Randomly select a host for false packet. Place result in IPv6 destination host address field
660
Does selected host address satisfy minimum hop requirement in Field C ?
No
662
Yes
664
Determine size (in bytes) of false packet body using value in Field F as a guide
Does false packet size satisfy minimum and maximum size requirements in Fields D and E ?
No
666
Yes
Fill in the packet body with random values
668
Set all extension header field values to zero. Copy saved values for Fields Ø, B, C, D, E, H, I, J, K, L, M, and N from original packet to new extension header in outbound false packet
670
B
B
672
Place value Ø1 in Field A of false packet, decrement X by 1
674
Encrypt extension header. Complete remainder of IPv6 message headers and processing and transmit new false packet
676
Is X = Ø ?
No
Yes
612
If value in Field K = 1, decrypt true packet body in reverse order in which encryptions were performed, using the value in Fields Ø and N to determine the end of the extension header. The decryption pointer used for the sender is given by the value in Field G
C
614
Pass decrypted message to TCP level of the message management stack
DONE

Fig. 6

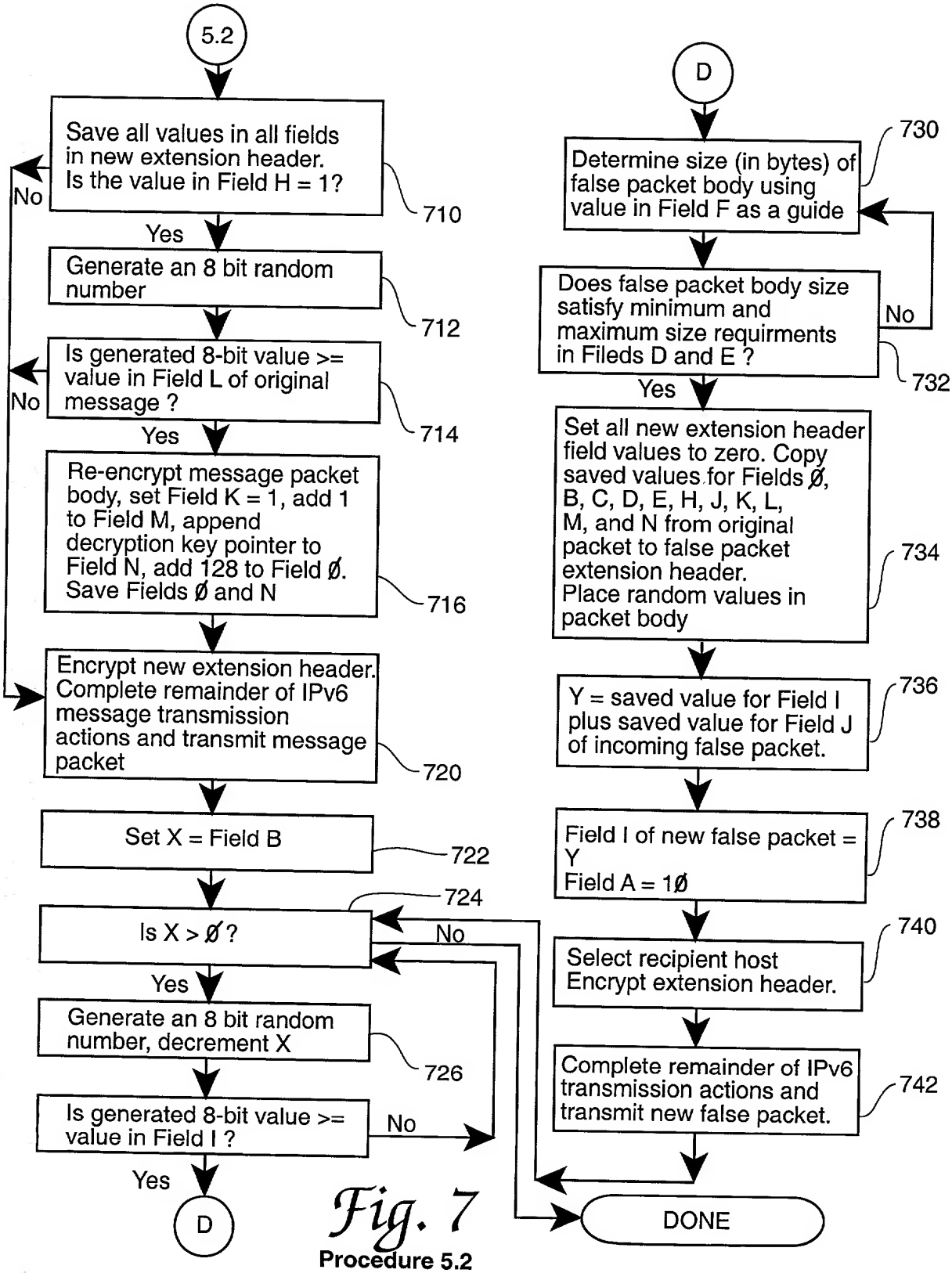

Fig. 7
Procedure 5.2

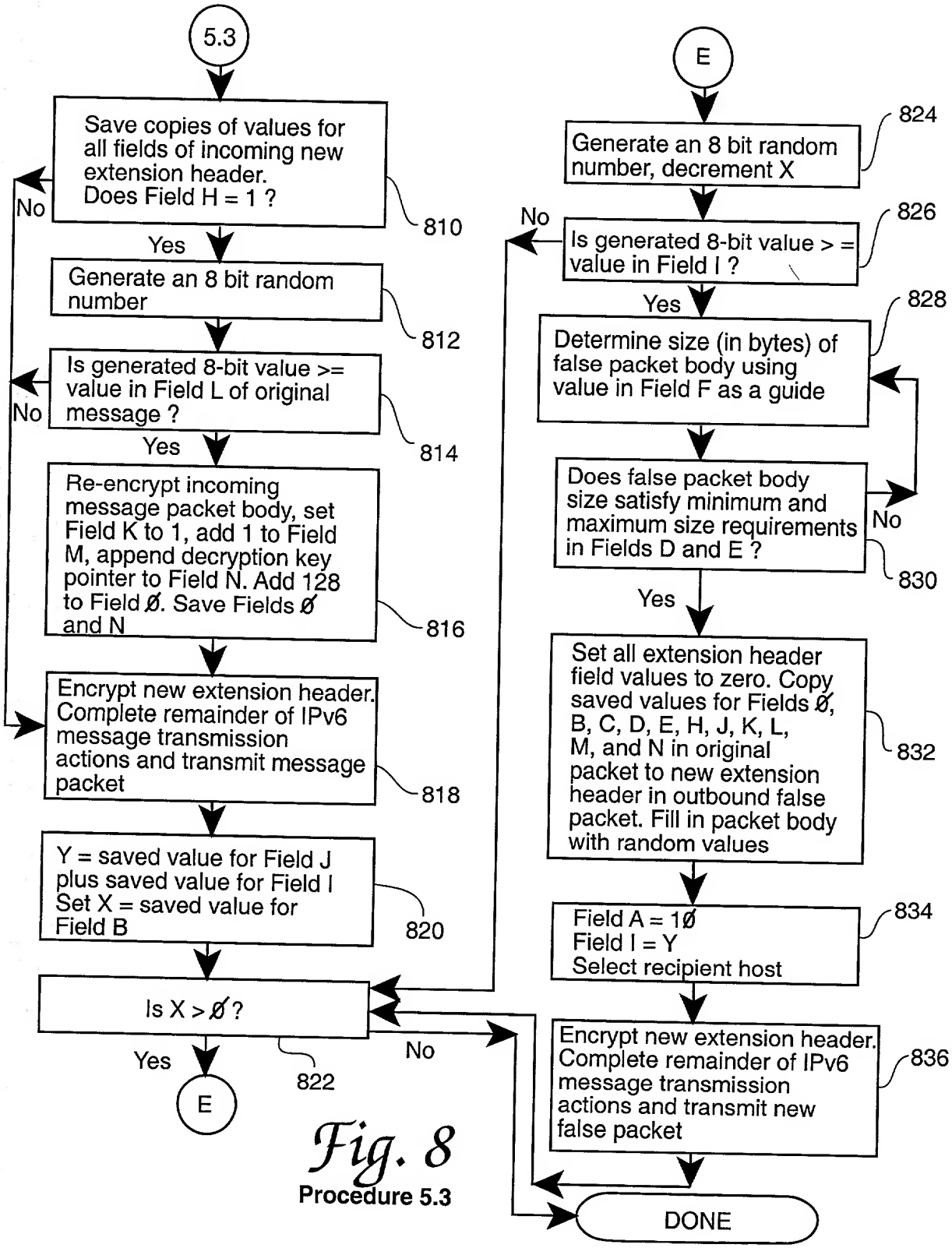

Fig. 8
Procedure 5.3

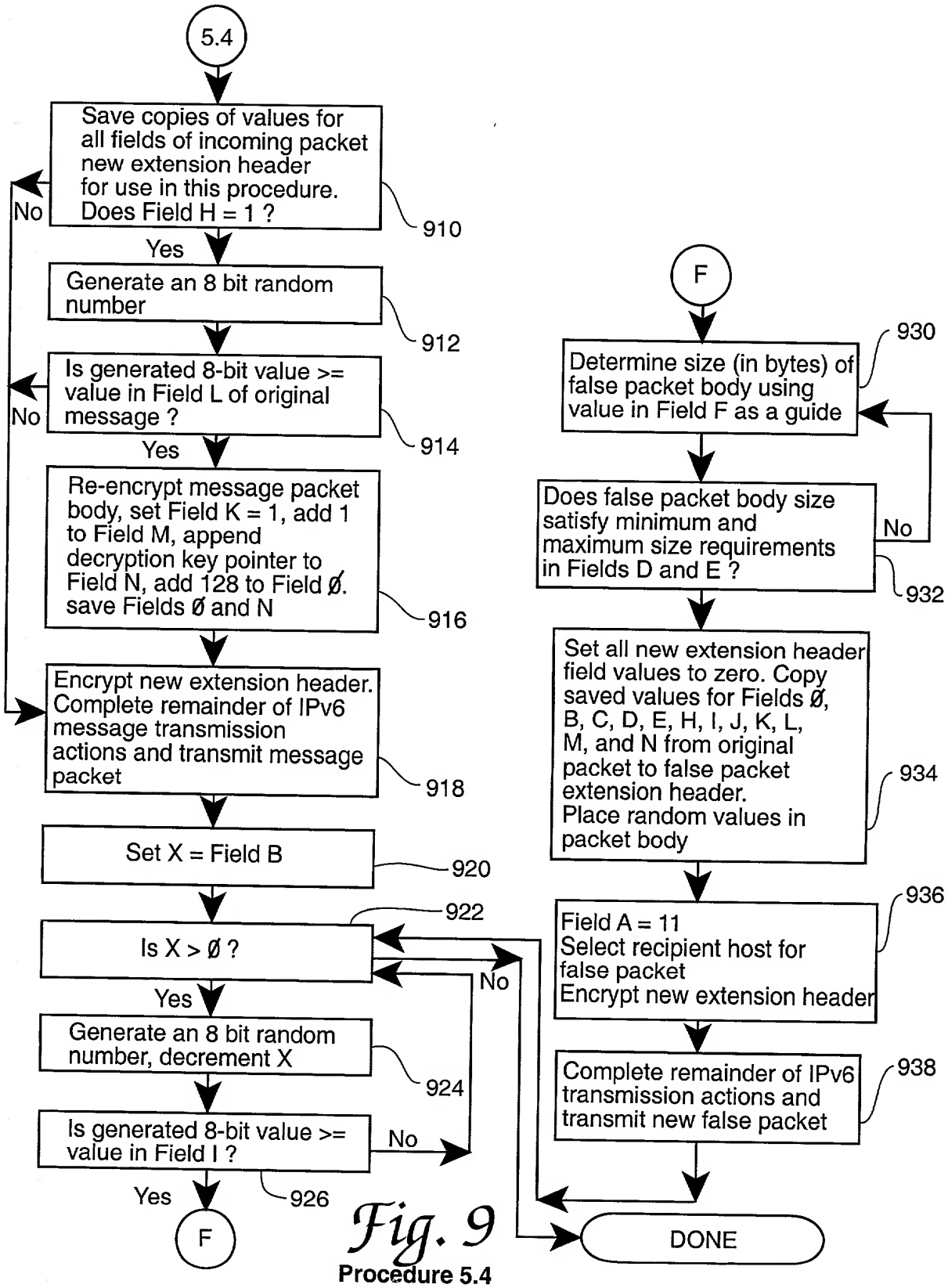

Fig. 9
Procedure 5.4

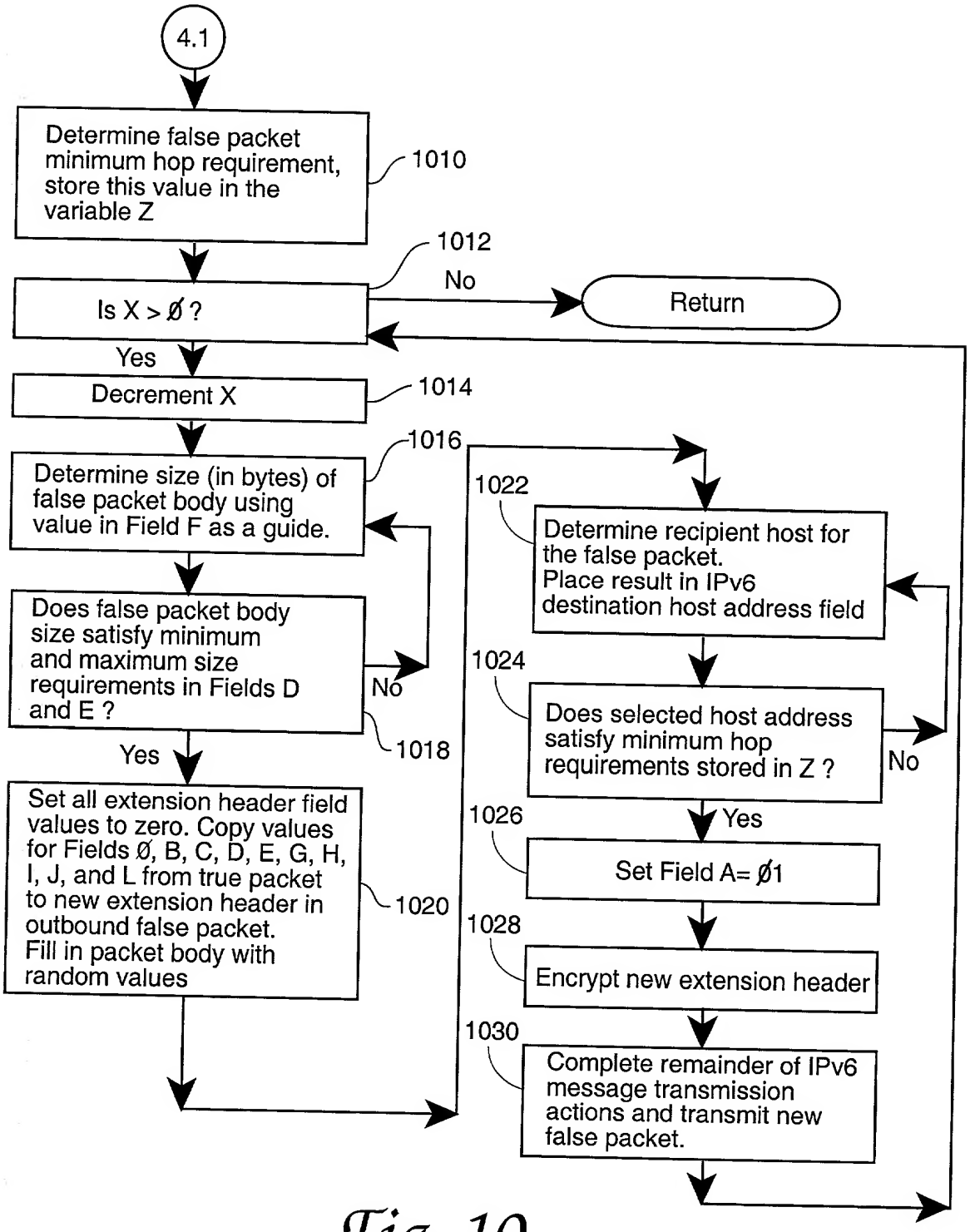

Fig. 10

Procedure 4.1